Interoperability of Databases and Interstate Trust: a Perilous Combination for Fundamental Rights

Evelien Brouwer 2019-05-25T13:24:38

On 14 May 2019, the Council adopted two regulations, Regulation 2019/817 and Regulation 2019/818, establishing a framework for the interoperability between EU information systems in the Area of Freedom, Security, and Justice. The new rules on interoperability, upon which the European Parliament agreed in April 2019, will allegedly provide for easier information sharing and 'considerably improve security in the EU, allow for more efficient checks at external borders, improve detection of multiple identities and help prevent and combat illegal migration'. All this, according to the press release of the Council, 'while safeguarding fundamental rights'. It is questionable whether this commitment made by the EU legislator is justified. Interoperability only 'works' as long as the reliability and trustworthiness of data in the databases involved are sufficiently guaranteed. Considering the number of states and the large-scale databases involved, the consequences of decision-making based incorrect or even unlawful data will be detrimental not only for the protection of fundamental rights but also for the effectiveness of interoperability as a data and border surveillance tool as such. Focusing on fundamental rights, I will argue in this contribution that 'interoperability' combined with 'interstate trust' is a perilous combination if this would allow national authorities to rely on data stored in EU data systems, instead of making a careful examination of each individual case. Despite formal safeguards in the regulations and the applicable data protection standards, it will be hard for data subjects to oppose decision-making based on incorrect data, when the source or the author of that information is unknown or when states can 'hide' behind the back of interstate trust without providing access to effective legal remedies. The problems which may arise for individuals through the 'blind' use of large-scale databases will be illustrated with two recent case-studies: the first concerns the entry of a human rights activist into SIS II, and the second one the reliance on Eurodac to determine the age of a minor asylum seeker. Considering the extensive scale of data processing, the fact that interoperability affects mainly third-country nationals, and because of the complexity of rules, it will be argued that the adopted instruments fail to meet the standards defined by the CJEU and the ECtHR on the basis of the rights to privacy and data protection.

Interoperability and multipurpose use of EU large-scale databases

Both Regulation 2019/817 which applies to information systems in the field of borders and visa and Regulation 2019/818 on systems in the field of police and

judicial cooperation, asylum and migration, build on the same interoperability components, which include:

- A **European search portal**, allowing competent authorities to search multiple information systems simultaneously, using both biographical and biometric data.
- A **shared biometric matching service**, enabling the searching and comparing of biometric data (fingerprints and facial images) from several systems.
- A **common identity repository**, which contains biographical and biometric data of third-country nationals available in several EU information systems.
- A **multiple identity detector**, to check whether the biographical identity data contained in the search exists in other systems covered, to enable the detection of multiple identities linked to the same set of biometric data.

The interoperability structure is thus based on a network or a mechanism through which different authorities can check whether information on a particular individual is available in one of the current (and future) EU databases. This search will be facilitated by the use and storage of biometrics in the different databases. The databases which can be connected via interoperability are numerous. They include the existing large-scale databases Schengen Information System or SIS II, Eurodac, and Visa Information System (VIS), and the Europol and Interpol databases. Furthermore, the interoperability scheme applies to the following systems when operational: the Entry Exit System (EES), the European Travel and Authorisation System (ETIAS), the European Criminal Record Information System on third-country nationals (ECRIS-TCN).

With the aforementioned common identity repository including biometric and 'biographical' data, the interoperability rules only involve a centralized database with regard to third-country nationals. According to the European Commission in the explanatory memorandum to the proposal, this differentiation between EU citizens and third-country nationals is justified by the aim of preserving security in the EU: 'Whilst not directly affecting EU nationals […], the proposals are expected to generate increased public trust by ensuring that their design and use increases the security of EU citizens.'

Multipurpose access to centralised databases

According to the press release, the interoperability systems will not 'modify the rights of access as set out in the legal basis relevant for each European information system, but will ease and improve information sharing'. Here the legislator has a point as it was not even necessary to extend access to the different databases involved for further purposes: this was already provided for in the various laws adopted in the last few years. In 2015, Eurodac, an administrative system with data on asylum seekers in the EU set up for the implementation of the Dublin system, has been extended for law enforcement purposes on the basis of Regulation 603/2013. VIS, including data on all applicants for short-term visas, has been developed as a multipurpose tool from the start, and also the new border systems ETIAS and EES will be accessible for law enforcement and security purposes. And the inclusion of biometric data in SIS III on the basis of the Regulation 2018/1861 for the purpose

of border control and the Regulation 2018/1862 in the field of police and judicial cooperation already changed the structure of SIS II into a more general investigation tool.

Vice versa, the ECRIS-TCN, a database which was presented as necessary for the purpose of judicial cooperation, will be accessible for immigration control purposes. ECRIS-TCN on which the Council and the European Parliament reached agreement in April 2019 provides for a centralized system with data on all third-country nationals with criminal records in the EU. In accordance with Article 7 of the ECRIS-TCN Regulation 2019/816 the information stored on previous criminal convictions on third-country nationals can be requested for criminal proceedings 'or for any other of the following purposes, if provided under and in accordance with national law.' Despite early and serious concerns of the Fundamental Rights Agency (FRA) against the use ECRIS-TCN for national immigration law purposes, the adopted Regulation now explicitly defines as one of the 'following purposes': 'visa, acquisition of citizenship and migration procedures, including asylum procedures'. This implies that ECRIS-TCN data can be used not only for rejecting short-term visa, but also for the refusal or withdrawal of residence permits of third-country nationals. The FRA warned against these secondary effects from national convictions based on previous irregular entry or stay, specifically for refugees and children and referred to the differentiated practices in the Member States with regard to criminalization of irregular stay and entry. According to the Commission in the explanatory memorandum to the 2016 proposal, the extent to which criminal record information is processed for other purposes would be 'a matter of national law'. Therefore, limitations to this further use would not be possible in the ECRIS-TCN proposal. The adopted rule in the interoperability Regulation shows that the legislator is not only aware, but also approves that Member States will use information on criminal records in the ECRIS-TCN for immigration law purposes, even if these decisions are based on the (possibly very different) criminal law systems of other states.

The case of a human rights activist in SIS II

On 13 August 2018, Lyudmyla Kozlovska, Ukrainian national, President of the Open Dialog Foundation (ODF) and married to a Polish citizen, was detained by the Belgian authorities following a passport control at the Brussels airport on the basis of a Polish alert in the SIS II for the purpose of refusal of entry or stay. The next day, the Belgian border authorities deported her to Kiev, Ukraine. Prior to the issuing of the SIS alert, Kozlovska was legally resident in Poland and had applied for an EU long term residence permit. During that procedure, she was informed by the Polish authorities that she was not listed in the SIS II. In the period following her expulsion from Belgium, Mrs Kozlovska was allowed to visit several Schengen states (including Belgium and Germany) for several days to talk with members of the European Parliament and national parliaments, despite the fact that the Polish alert was not withdrawn. In March 2019, the Belgian authorities provided her with a five year residence permit, after which decision Poland is obliged to withdraw the SIS alert in accordance with the Schengen rules. In E., addressing the obligation of consultation between Member States in these matters related to SIS, the CJEU confirmed that an individual has the right to rely before courts on the obligation

to withdraw an alert from SIS if that is the outcome of this consultation. Access to legal remedies against the Polish alert is however difficult, also because she has never been informed about the precise reasons for the SIS alert. Furthermore, until the SIS alert is deleted, Mrs Kozlovska risks to be denied entrance or expelled by other Schengen states. Her case illustrates what happens if national authorities 'blindly' rely on data in EU databases and the effect of these decisions for human rights, including the right of freedom of expression, freedom of movement and effective judicial protection. Even if in the end she obtained a residence permit by one state, it will remain difficult to get rid of this 'digital entry ban'. It is to be feared that interoperability will only enhance this informational bureaucracy, affecting the effective protection of fundamental rights.

The case of a minor unaccompanied asylum seeker in Eurodac

In May 2019, the Dutch radio-programme (VPRO) broadcasted a documentary on a case of a minor asylum seeker who, when entering EU territory via Italy, was registered into Eurodac as being an adult by the Italian authorities. Traveling further north, she applied for asylum in the Netherlands where she informed the immigration authorities (IND) she was 15. The IND however refused to treat her as a minor relying on the data in Eurodac on the basis of the principle of interstate trust. Because of this refusal the minor did not receive further protection even though during the procedure she substantiated her age with documents and, as her lawyer submits in this documentary, from sight and behaviour, she clearly is a minor. This Dutch policy of relying on Eurodac on the basis of the principle of interstate trust without any further investigation in to the age of the minor, has been approved by the Dutch highest administrative court (ABRvS). In aforementioned case, the minor herself had lied about her age to the Italian authorities in fear of being separated from the group with which she entered Italy. But in the documentary officials of IOM and UNHCR confirm that incorrect registration of age of minors in Eurodac is common practice. A wrong birth date can be registered into Eurodac in periods of chaos when large numbers of asylum seekers arrive, but sometimes also on the basis of miscommunication or lack of information provided to minor asylum seekers. As the report Digital Identity in the Migration and Refugee Context shows, during the identification process of migrants and refugees, the protection of privacy, informed consent and data protection are often compromised, not only for minors. The specific problems of children in registration procedures for immigration purposes were also established in the report Under watchful eyes of the FRA. Dealing with the collection of data during visa applications or for the purpose of the Dublin system, the FRA found that rights of children were affected in different ways, dealing with child-unfriendly treatment, doubts with regard to the quality and reliability of fingerprints, and risk of re-traumatization. Where interoperability might be a tool to trace missing children, the FRA in a report of 2017 underlined rightfully that this is only the case if Member States will make more use of the existing possibility to report missing children into SIS II and improve cooperation between their national authorities.

Why perilous?

The first reason why interoperability of databases combined with interstate trust may have serious human rights and accuracy implications is the wide extent of the use of the stored into information. Large-scale databases are large-scale databases: they contain millions of data sets on individuals and they are used by a high number of national authorities, with different tasks and powers. This means that incorrect or outdated information in one of the aforementioned databases has a high risk of being multiplied in other EU databases and at the national level. For example, Eurodac, used by 32 EU and non-EU states, at the end of 2017 included more than 5 million 'fingerprint datasets'. More than one million transactions to Eurodac took place in 2017, with a peak in February 2017 of 6.000 transactions a day. For the purpose of law enforcement, 550 Eurodac searches were performed by the 'designated authorities' of Member States and 114 by Europol. At the end of 2018, SIS II contained more than 82 million alerts of which almost a million alerts were on persons. SIS II in 2018 was accessed more than 6 billion times by Member States and Associated Countries, representing an increase of 20% compared to 2017. In 2018, 267.239 foreign hits were reported of which 77% were triggered by alerts on persons. And finally VIS, accessible by 26 states (EU and non-EU Member States), contained at the end of 2017 about 49 million visa applications and 42 million fingerprints sets.

Second, the effects of interoperability will in the first place affect third-country nationals. As pointed out by the EDPS in Opinion 4/2018, the interoperability regulation in itself create a new centralised database containing information about millions of third-country nationals, including their biometric data. The consequences of any data breach could seriously harm a potentially very large number of individuals and, according to the EDPS, if 'such information ever falls into the wrong hands, the database could become a dangerous tool against fundamental rights'. The risk of misuse of data is a risk which addresses the heart or 'essence' of the right to private life and data protection, protected in Article 8 ECHR and 7, respectively 8 of the Charter on Fundamental Rights. Both the CJEU and the ECtHR have repeatedly warned in their case-law against the unrestricted or disproportional processing and use of personal information. In *S. and Marper v. UK*, the ECtHR warned against the risk of stigmatisation where information on large groups of unsuspected citizens is stored into centralised databases for law enforcement purposes. One of the criteria in *Digital Rights Ireland* for the CJEU to find the Data Retention Directive in violation of the right to privacy and data protection, concerned the fact that its implementation would entail the data processing of 'practically the entire European population', also involving persons without any link to criminal prosecution. And in *Schwarz v. Bochum*, the CJEU found that the Passport Regulation 2252/2004 did not amount to violation of the rights protected in 7 and 8 of the Charter, because it only provided for the recording of two fingerprints and facial image on the passport, it did not prescribe a central storage of the data of passport holders, and the purpose of the use of the data was limited to identification of the owner and verification of the authenticity of the document and would not be used for other purposes. These criteria are relevant when assessing the use of large-scale databases and the effects of interoperability, especially where these measures

primarily address third-country nationals. Discretionary national powers and the availability of mobile devices will make it possible to check individuals not only at the borders, but also within the national territory. The risk of discriminatory checks within the EU borders is enhanced, as pointed out by Vavoula in her eumigrationlawblog, by Article 20 of the Regulation 2019/818 according to which police authorities can check the aforementioned CIR or Common Identity Repository solely for the purpose of identification of a person, for example if 'a person is unable or refuses to cooperate'. This entails the risk of extensive use of databases, in violation of the strictly necessity test as defined by the CJEU in Digital Rights Ireland and Schrems and emphasised in the EDPS toolkit on assessing the necessity of data processing. The fact that interoperability and the centralization of data bases mainly affect third-county nationals (or EU citizens with a third-country nationality as in ECRIS-TCN) fails to respect the fundamental right to non-discrimination.

Third, there is a problem of transparency of powers. As underlined by the EDPS in the aforementioned Opinion 4/2018, the interoperability regulations only add another layer to the complexity of practices and laws of existing data systems. The extensive number of instruments dealing with data processing, with each their own set of data protection rules, in combination with the general rules in the GDPR and the Data Protection Directive, does not result in a very transparent legal framework. This complexity of rules also triggers questions on accountability and liability with regard to incorrect or unlawful data processing. If more databases and users are involved, it will be hard for the data subject to understand not only which particular law applies, but also which state or organisation should be addressed with regard to using their rights to access, correction or deletion of data, and, finally, their right to effective judicial protection. This lack of transparency is not only a problem for data subjects. Effective enforcement of data protection rights is indispensable to ensure the accuracy and legitimacy of data processing by Member States and thus to attain the goals of the Area of Freedom, Security and Justice.
